Future (/Future)

India comes on the crosshairs of cryptojackers; even conglomerates targeted

Shadma Shaikh (https://factordaily.com/author/shadma/) | February 20, 2018 | 7 min

(https://www.[illegible]text=India%20con[illegible]u=https%3A%2F%2F[illegible]

Story Highlights

- Smokescreen has identified 4 large customers with networks as large as 1000 computers being attacked by malware that mines cryptocurrency.
- Banbreach has discovered popular websites likely hit by a malware mining Monero in background using visitor's computing power.
- Check Point has discovered 3 variants of cryptomining malware with Coinhive a script for mining Monero impacting more than 1 in 5 orgs

Nearly half a dozen Indian websites that serve up millions of hits every month have been infected by a malware that hogs processing power of a visitors' computer to mine cryptocurrencies.

But that's not all. Malware that mines cryptocurrencies have started spreading on enterprise networks owned by large manufacturers in India and security professionals anticipate that targeted attempts at infecting Indian computers could be on the rise.

"India is a highly attractive and vulnerable market for large crypto mining operations given the sheer number of computers that are up and running at any given point," said Rohit Srivastwa, senior director at security solutions company Quick Heal.

India could be turning into a new target for global cryptocurrency malware campaigns where large enterprise networks and popular websites unwittingly mine cryptocurrencies for attackers.

"Overall, we received over 14 million hits of cryptocurrency miners on our users' machines. Among these, PE executable miners contributed about 3 million and more than 10 million of script miners were detected," wrote Quick Heal in its Annual Threat Report of 2018 about the trends noted of the year gone by. PE executables are portable executable files often targeted by malware to invoke malicious actions on a computer.

One way to own a cryptocurrency is to buy it. The other is to mine it. Yet another way of acquiring cryptocurrency is to steal it. To steal them, you could orchestrate massive hacks, or let loose a low-risk malware campaign that's capable of mining cryptocurrencies. This practice is more popularly known as cryptojacking.

These malware attacks often hijack the host's computers to mine for cryptocurrencies. Or they could be embedded on websites to mine cryptocurrencies using a visitor's computer. It's like hacking your neighbor's wifi password to pilfer bandwidth.

The chief information security officer of one of India's largest multinational conglomerate recalls a recent security attack on their network: "It looked like a worm that was trying to replicate itself and move laterally through the network," he said, requesting anonymity. The worm, it turned out, was a crypto miner that was slowing their systems, since it was using the system's processing power to mine Monero, a cryptocurrency that's growing in popularity.

"You have to think about the scale of this," says Sahir Hidayatullah of Smokescreen, another security solutions provider. "If you are infecting thousands of machines and they

Rohit Sriwastva, senior director, Quickheal

are working for you 24/7, mining currency in the background for months, it adds up significantly."

In the last month alone, Hidayatullah's company has been called in by four of its large customers, including large manufacturers and financial services company, to take a closer look at incident reports. "The companies called us for incident response where they found malware running crypto mining," he says.

The manufacturing sector is an easier target. "You think the textile manufacturers who have 100 to 500 computers running will ever notice that their system is slow because it could be mining bitcoins in the background? Some customers had been infected and were mining for the attacker for over 6 months," he says.

Large enterprise security firms including FireEye and Check Point have found different variants of crypto mining malware impacting organisations globally. India is already big on the radar of attackers.

Earlier this month, Suman Kar, the founder of Kolkata based BanBreach identified crypto mining malware on half a dozen websites

Sahir Hidayatullah, CEO Smokescreen

(https://twitter.com/Banbreach/status/960199133016612865), including that of Deccan Chronicle and Asian Age, Punjab National Bank's Institute of Information Technology, IT hardware marketplace theITDepot.com, Karnataka Industrial Area Development Board's website and Indiangovtjobs.in.

These websites were running an unauthorised script from Coinhive, an in-browser crypto miner that's otherwise used by site owners as an alternate revenue channel.

Kar tells us that his team wrote to Deccan Chronicle about the bug. The media house did not respond to his email but deleted the Coinhive script the following day. Here's where it gets interesting. The script was back up on the site just a few hours after it was deleted. Kar figures that the media house had not been secretly mining Monero but was likely infected by a malware.

"They might have deleted an instance of the Coinhive script but they probably did not remove it from source," Kar said. Malware can be programmed to reinject itself.

FactorDaily wrote to Deccan Chronicle's IT team to get clarity on how it handled the issue but had not received a response from them at the time of publishing this story.

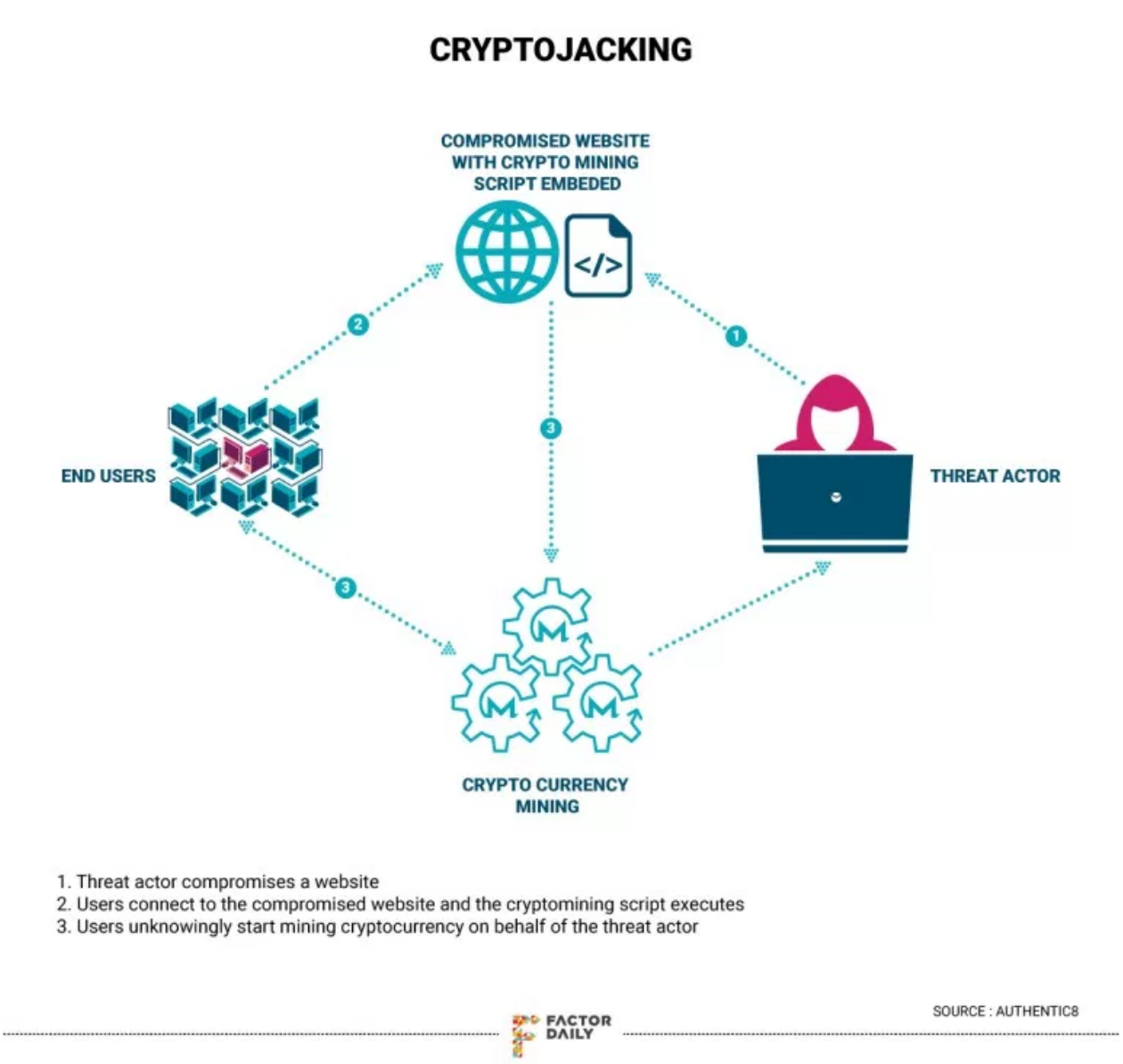
The infamous Coinhive based attacks

At least three variants of cryptomining malware made it to the list of top 10 most prevalent malware list published (https://www.checkpoint.com/press/2018/januarys-wanted-malware-cryptomining-malware-continues-drain-enterprise-cpu-power-say-check-point/) by Check Point in January. Of them, Coinhive based malware ranked the highest, impacting more than one-in-five organizations.

Coinhive was originally conceived as a legitimate business use-case for websites, as an alternative to ad-based revenue channel. It has now gained the reputation of crypto jacker's go-to tool. The site has seen over 150,000 signups. The Coinhive script mines Monero coins when a user visits a web page. The embedded script uses computational resources of the visitor's machine to mine coins, impacting system performance.

Last week, Scott Helme, a security researcher and founder of securityheaders.io had found around (https://scotthelme.co.uk/protect-site-from-cryptojacking-csp-sri/) 4,200 global websites that had been compromised by a crypto mining Coinhive script invoked through a third-party plug-in called Browsealoud.

Browsealoud is a web screen reader created for people with visual impairments and is embedded in more than 4,000 websites, many of which belong to governments. By compromising Browsealoud, attackers gained access to the websites that used the plugin.



Coinhive markets itself as a legitimate approach to mining. There is nothing unethical about running a Coinhive script on a website, except that it's important to tell your visitors that their computers are being used to mine cryptocurrency.

"We believe that In-Browser mining could be a viable alternative to micropayments," a Coinhive representative wrote in response to an email query to FactorDaily. "While many websites still use our miner in 'unimaginative' ways, best practices are slowly emerging. This is all new technology and we still have a lot to learn," the representative said.

In the case of the 4,200 websites discovered by Helme or the ones discovered by Kar, the visitors were uninformed of the presence of a Coinhive script using their computing power.

Check Point said in a press release that crypto mining malware continues to impact organizations globally as 23% of them were affected by the Coinhive variant during January 2018.

Is Monero mining worth it?

The Browseloud plugin attackers earned only $24, according to a report (https://motherboard.vice.com/en_us/article/vbpbz4/creators-of-in-browser-cryptocurrency-miner-coinhive-say-their-reputation-couldnt-be-much-worse) by MotherBoard. However, a new report (https://blog.checkpoint.com/2018/02/15/crypto-miners-now-target-jenkins-servers/) by Check Point says that a hacker group made over $3 million by breaking into Jenkins, a popular and largely used open-source automation server.

With just 10-20 active miners on your site, you can expect a monthly revenue of about 0.3 XMR (~$96), Coinhive explains on its website. Top Coinhive users who have been at it since the start (September 2017) have mined over 1000 XMR (~$323,338) each, said the email from Coinhive. Then there's also the likelihood of Monero, like Bitcoin, appreciating over time.

But crytojacking incidents are not limited to browser-based attacks. Large network attacks targeted at enterprise verticals like manufacturing, financial and IT services have seen a fair share of the rise in countries like India. The malware behind the attacks identified by FireEye and Smokescreen are highly sophisticated multistage malware. As the name suggests multistage malware works in different stages with different intents.

Cybercriminals wouldn't spend their time to write such complex malware if the monetary value wasn't significant, says Hidayatullah of Smokescreen. There are easier ways to monetize once they get on your system, like stealing your credentials and selling it on the dark web.

"We've observed one threat actor mining around 1 XMR/day (~$320.58/day), demonstrating the potential profitability and reason behind the recent rise in such attacks," the FireEye blog post (https://www.fireeye.com/blog/threat-research/2018/02/cve-2017-10271-used-to-deliver-cryptominers.html) states.

Victimless Crime or larger threat?

Is an incident of crypto jacking at a manufacturing unit with about 100 computers scary enough to keep their CISO awake at night? Probably not. Systems slowing down is one of the largest visible impact of crypto jacking, but it also one of the smaller problems in the larger scheme of things. Also as an internet user what's it to me if I visit some sites and it uses my computing power to mine currency?

On the surface, crypto jacking looks like a simple crime. A script running in the background of a large infected network could go unnoticed for months together but is easy to fix once it's found. But cybercriminals who are sophisticated enough to write multi-stage malware often do not stop at small exploits. A cybercriminal whose malware sits on these infected systems mining for months is very likely to pull out other information from the system, like corporate credentials, or for example, eBay login or Amazon gift card.

Updated at 02:44 pm on February 22, 2018 to add details from Quick Heal's Annual Threat Report.

Disclosure: FactorDaily is owned by SourceCode Media, which counts Accel Partners, Blume Ventures and Vijay Shekhar Sharma among its investors. Accel Partners is an early investor in Flipkart. Vijay Shekhar Sharma is the founder of Paytm. None of FactorDaily's investors have any influence on its reporting about India's technology and startup ecosystem.

cybersecurity (https://factordaily.com/tag/cybersecurity/)

Monero (https://factordaily.com/tag/monero/)

(https://factordaily.com/zcash-founder-zooko-wilcox-interview/)

Jayadevan PK (https://factordaily.com/author/jayadevan-pk/)

The man building a 'better Bitcoin' on why Bitcoin isn't the cryptocurrency for mainstream use (https://factordaily.com/zcash-founder-zooko-wilcox-interview/)

February 13, 2018

FUTURE (/FUTURE)

(https://www.[illegible]text=The%20man%20building%20a%20better%20Bitcoin%20on%20why%20Bitcoin%20isn't%20the%20cryptocurrency%20for%20mainstream%20use&u=https%3A//factordaily.com/zcash-founder-zooko-wilcox-interview/)

(https://factordaily.com/cryptocurrency-trading-india-government-clampdown/)

Anand Murali (https://factordaily.com/author/anand/)

Cryptocurrency party continues despite India clampdown (https://factordaily.com/cryptocurrency-trading-india-government-clampdown/)

January 8, 2018

FUTURE (/FUTURE)

u=https%3A%2F%2Ffactordaily.com%2Fcryptocurrency-party-continues-despite-India-clampdown%2F&title=Cryptocurrency%20party%20continues%20despite%20India%20clampdown&summary=Here%20is%20an%20interesting%20story%20for%20you!&source=FactorDaily

(https://factordaily.com/bitcoin-india-sykam-reddy-users-account-blocked/)

Anand Murali (https://factordaily.com/author/anand/)

Crypto traders miffed as Bitcoin India locks their accounts; platform says resolving issue (https://factordaily.com/bitcoin-india-sykam-reddy-users-account-blocked/)

December 22, 2017

FUTURE (/FUTURE)

(https://factordaily.com/bitcoin-regulation-pil-supreme-court/)

Anand Murali (https://factordaily.com/author/anand/)

Two young Indians turn to Supreme Court to make laws around Bitcoin, cryptocurrencies less turbid (https://factordaily.com/bitcoin-regulation-pil-supreme-court/)

November 24, 2017

FUTURE (/FUTURE)

1 Comment Sort by **Top**

Add a comment...

Liya Minisk · Московский государственный университет имени М.В.Ломоносова

Check this link [http://your-numerology-2018.club] to see Numerological report which changed my life, family relationships, career and more ! I dont believe it until now, but I want to share this with EVERYONE, because it works!

P.S. people say that this information is just mind-blowing at first, ha-ha 🙂

Like · Reply · 1w · Edited

Facebook Comments Plugin

(https://facebook.com/factordaily) (https://twitter.com/factordaily)

(https://www.instagram.com/factordaily/) (/feed)

hello@factordaily.com (mailto:hello@factordaily.com)

Code of Conduct (https://factordaily.com/code-of-conduct/)

FactorBranded (http://factorbranded.com)

About Us (https://factordaily.com/about/)

Contact Us (https://factordaily.com/contact/)